REMARKS

Reconsideration of the application in view of the above amendments and the following remarks is respectfully requested.

Rejections of the Claims Under 35 U.S.C. §§ 102 & 103

In the Office Action dated August 11, 2003, claims 1-2, 5-6, 11-12, 15-16 and 21 were rejected under 35 U.S.C. § 102 as being unpatentable over US Patent 6,237,096, issued to Bisbee et al. (hereafter referred to as "*Bisbee et al.*"). Claims 3-4 and 13-14 were rejected under 35 USC § 103 as being unpatentable over *Bisbee et al.*, in view of "An Introduction to database Systems", by C. J. Date) (hereafter referred to as "*Date*"). Also, claims 9-10 and 19-20 were rejected under 35 U.S.C. § 103 as being unpatentable over *Bisbee et al.* Finally, claims 7-8 and 17-18 were rejected under 35 U.S.C. § 103 as being as being unpatentable over *Bisbee et al.*, in view of US Patent 6,233,577.

Overview of The Claimed Invention:

A digital signature service is integrated into a database. The digital signature service provides to a user seamless integration between executing digital signature functions on data, and storing that data in a database. In one embodiment, the digital signature service is integrated within the database management system, such as a relational database management system ("RDBMS"). A database client, such as an application program, generates data for storage in a database record. Specifically, the database client generates a command to the RDBMS to execute a store procedure that digitally signs the data and that saves the data in a persistent datastore. In response to the command, the RDBMS, using a digital certificate for the user, generates a signature from the data. In addition, the RDBMS generates a digital signature object for the data that includes the data, certificate and signature. The digital signature object is stored in the database.

The digital signature service also permits a user to verify digital signatures stored in the database. For this function, the RDMS receives a query command from the user to retrieve the data from the record of the database. In response to the query command, the RDBMS retrieves the digital signature object containing the data, certificate and signature. The RDMS processes the data and the certificate, using the signature, to verify that the data and the certificate are unaltered from their original contents. The RDBMS also obtains, from the certificate, an authentication of the digital signatory. After the digital signature verification, data is provided as a response to the query command. The digital signature service implements business logic to retrieve data based on digital signature criteria, and implements filter functions to filter the storage and retrieval of data based on verification and authentication of digital signatures. Furthermore, the digital signature service permits multiple signatories on a single data item.

A. The Cited References Do Not Disclose Directly Integrating A Database Store Procedure With A Digital Signature Service.

Amended claim 1 recites:

A method for integrating a digital signature service into a database, said method comprising the steps of:

storing a database comprising a plurality of records;

receiving a store procedure with data from a client of said database;

in response to said store procedure,

receiving a digital certificate for said client;

receiving a private key for said client;

generating a signature from said data, digital certificate and private key of said client;

generating a signature object for said data, said digital signature object comprising said data, certificate and signature; and

storing said signature object as at least a portion of one of said record in said database.

Thus, amended claim 1 sets forth a method for generating a signature in response to a store procedure and storing the signature, in the form of a signature object, in a database record.

In support of the rejection of claims 1, 11 and 21, the Examiner cites the procedure for *Bisbee et al.*'s document authentication system. (Col. 6, line 46-54, Col. 6, lines 60-63, Col. 7, lines 5-8, Col. 3, lines 9-14, and Col. 3, lines 16-19). As discussed more fully below, none of the references, either alone or in combination, teach generating a signature in response to a store procedure and storing the signature, in the form of a signature object, in a database record.

1. The Transfer Agent Of *Bisbee et al.* Does Not Store A Digital Signature In A Database.

Bisbee et al. do disclose signing a document for a client (referred to in *Bisbee et al.* as a "Transfer Agent"). However, the signed document is not stored in a database. Instead, the signed document is transmitted to the Authentication Center for storage. With regard to signing a document, *Bisbee et al.* disclose:

> As described below, the Transfer Agent provides the document in digital form, such as the output of a conventional word processor, to the Transfer Agent's Token. ... The digital document is digitally signed and/or encrypted by the DAS Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically. (e.g., by modem or computer network). (Col. 6, lines 46 – 55).

Accordingly, *Bisbee et al.* do not anticipate the claimed invention because *Bisbee et al.* disclose transmitting the signed document to the Authentication Center. As such, Bisbee et al. do not disclose generating a signature in response to a store procedure and storing the signature in a database record.

2. The Authentication Center Appends A Digital Signature To A Previously Signed Document.

Claims 1, 11 and 21 recite limitations to generate a signature from data, digital certificate and private key of the client. In contrast, the Authentication Center signs a previously signed document, signed by the Transfer Agent, and appends that digital signature to the originally signed document. Specifically, *Bisbee et al.* disclose the process at the Authentication Center as:

> The Authentication Center verifies the identify of the Transfer Agent and the authenticity of the documents, and *appends* a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (Col. 6, lines 60 – 64, emphasis added).

The Authentication Center signs a previously signed document with the certificate of the Authentication Center. In the claimed invention, the certificate of a database client is used to sign the original document. Accordingly, because *Bisbee et al.* teach signing a previously signed document, *Bisbee et al.* do not anticipate the claimed invention.

3. The Authentication Center Does Not Execute A Store Procedure To Store A Signed Document In A Database.

Amended claims 1, 11 and 21 include the limitations for executing a store procedure that invokes a process to sign a document and store the signed document in a database record. *Bisbee et al.* disclose storing the document at the Authentication Center:

> The authenticated, digitally signed and/or encrypted documents are stored by the third party Authentication Center in any convenient form, such as on optical and/or magnetic disks. (Col. 7, lines 5 – 8).

Thus, *Bisbee et al.* only disclose storing documents to permanent medium (*i.e.,* optical and/or magnetic disks) and do not disclose storing a signature object to records of a database. Therefore, for this additional reason, claims 1, 11 and 21 are not anticipated by *Bisbee et al.*

B. *Date* Does Not Mention A Digital Signature Service.

Date teaches basic database concepts. *Date* does not mention or suggest using a digital signature service in conjunction with a database store procedure. In order to render a combination obvious, there must be some suggestion to combine teaching. *Date* provides no suggestion to combine the teaching of a database with a digital signature service. Therefore, *Date* does not render the claimed invention obvious.

<u>Dependent Claims</u>:

Dependent claims 2-10 are depend, either directly or indirectly, upon independent claim 1, and therefore for the same reasons claim 1 is patentable over the cited reference, claims 2-10 are also patentable over the references. Similarly, claims 12-20 are directly or indirectly, dependent, upon claim 11, and therefore for the same reasons claim 11 is patentable over the cited references, claims 12-2- are also patentable over the references.

CONCLUSION

In view of the foregoing, it is submitted that the claims are in condition for allowance. Reconsideration of the rejections and objections is requested. Allowance is earnestly solicited at the earliest possible date.

Respectfully submitted,

STATTLER JOHANSEN & ADELI LLP

Dated: January 12, 2004

John Stattler
Reg. No. 36,285

Stattler, Johansen & Adeli LLP
PO Box 51860
Palo Alto, CA 94303-0728
Phone: (650) 934-0470 ext.100
Fax: (650) 934-0475